ABSTRACT

A fingerprints embedment system employing an anonymous fingerprinting method using a bilinear Diffie-Hellman problem includes three participants, introduces system parameters and generates a public key and a secret key of each of the first and the second participant. The anonymous fingerprinting method registers information on the first participant to a third participant based on the system parameters and the public and the secret key of the first participant, wherein the third participant issues a certificate based on the information of the first participant and authenticates a fairness of the first participant based on the certificate. Thereafter, the anonymous fingerprinting method embeds fingerprints into a digital content to be bought by the first participant and, when an illegal duplicate of the digital content or an illegally redistributed duplicate is found, identifies a traitor, which illegally duplicates the digital content or redistributes the illegally duplicated digital content, with the first participant.